Annual 47 C.F.R. 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date Filed: March 1, 2009

Company Name: TGEC Communications

Form 499 Filer ID: 816476

Signatory: M. Devin Semler

Title of Signatory: President

I, M. Devin Semler, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. (See Attachment 1)

The company has not taken any actions against data brokers in the past year. However, it is understood that the company must report any information that they have with respect to the processes individuals not associated to the customer's account or data brokers are using to attempt to access CPNI, and what steps the company is taking to protect CPNI. Furthermore, the company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signatory

3/1/2009

Date

PRESIDENT

Print Name - Signatory

TGEC Communications CPNI Privacy Statement and Protection Procedures

**Submitted in accordance to the FCC Annual 47 C.F.R. 64.2009(e) CPNI Certification Requirement*

CPNI is the individually identifiable information that is created by a customer's relationship with a communications provider, i.e. data regarding frequency, duration and timing of calls, including the information on a customer's bill and call-identifying information. The following statements detail how the company, TGEC Communications works to uphold its responsibility to protect customer information and meet FCC CPNI regulation requirements.

I. Carrier Authentication

The release of call detail information over the telephone presents an immediate risk to privacy; therefore, TGEC Communications will only release call detail information based on a customer initiated telephone call under three circumstances: (1) when a customer provides a pre-established password; (2) when a customer requests that the information be sent to the customer's address of record; or (3) when a carrier calls the telephone number of record and discloses the information and able to speak with the customer contact of record. In addition, TGEC Communications will continue to provide mandatory password protection for online account access. Furthermore, the company will not provide online access to CPNI based solely on the customer's biographical information provided to initiate service with the company.

II. Notice of Account Changes

TGEC Communications will notify the customer immediately via automated email notification of any account activity associated to a change in previously recorded customer account information, i.e. a change to an online password, creation of an online account or a change in an address of record. Should the customer not be reached via email the company will immediately forward the customer a letter to the billing address of record detailing the requested account changes and/or other requested CPNI information.

III. CPNI Storage, Maintenance and Security

TGEC Communications' IT Department has adopted many of the rules initiated by the PCI Data Security Standards Council (PCI DSS) to protect customer CPNI. The PCI DSS is a multifaceted security standard utilized by credit card companies that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard has allowed TGEC Communications to proactively protect customer account data. The following is a list of key items implemented to protect against a potential data breach:

1. Installed and maintained a firewall configuration to protect CPNI.
2. Prohibited use of vendor-supplied defaults for system passwords.
3. Mandatory username and passwords required for employees to review CPNI.
4. Restrict physical access to databases storing CPNI.
5. Constant monitoring of access to network resources storing CPNI.
6. Regularly test security systems and processes put in place to restrict access to CPNI.

IV. Notice of Unauthorized Disclosure of CPNI

In the event of a breach of CPNI, TGEC Communications' Regulatory Department will immediately notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) within seven business days via the CPNI Breach Reporting Facility found online: www.cpnireporting.gov. In accordance to FCC CPNI regulations the company will wait seven days after notifying the USSS and FBI before contacting affected customers to ensure these law enforcement institutions are allotted time for a thorough investigation. However, the company does reserve the right to notify its customers sooner should qualified company personnel interpret the breach as having potential or risk of immediate and irreparable harm to its customer base. Furthermore, in accordance to FCC CPNI regulations the company's Regulatory Affairs Department will keep records of discovered breaches for a minimum of two years.

V. Joint Venture and Independent Contractor Use of CPNI

TGEC Communications will first obtain opt-in consent from a customer before disclosing a customer's CPNI to a joint venture partner or an independent contractor for the marketing of communications-related services to the customer. This consent may be in the form of third party verification voice recording or within the customer's Letter of Agreement signed to initiate telecommunications services from TGEC Communications Both media will be maintained on file at the company's corporate headquarters for a minimum of two years after the customer initiates service with the company.

VI. Annual CPNI Certification

TGEC Communications will file an annual certification with the FCC, explaining any actions that the company has taken against data brokers and summarizing all consumer complaints that the company has received during the year related to the unauthorized release of CPNI. The company's annual CPNI certification will include an officer's signature attesting knowledge that the company's procedures are in compliance with the current FCC CPNI rules and regulations.